JOURNAL OF ALGEBRA, 2, 395-401 (1965)

Some p-Solvable Groups

E. C. DADE

Department of Mathematics, California Institute of Technology, Pasadena, California

Communicated by Graham Higman

Received November 10, 1964

As a result of their work on the properties of p-solvable groups, P. Hall and G. Higman were led to pose the following question [**2**]:

(0.1) *"If p is odd and not a Fermat prime, is it true that every p-soluble group of p-length l has subgroups H and K such that K is normal in H, and the factor group H/K is isomorphic with a Sylow p-subgroup of the symmetric group on p^l letters?"*

The answer to this question is no. For any odd prime p, we shall exhibit a class of p-solvable groups of p-length 3 having no such subgroups H, K.

1. PRELIMINARY LEMMAS

Our group will be the fifth term of a chain of groups $1 = G_0 \subset G_1 \subset \cdots$ satisfying:

(1.1) *For each $i \geqslant 1$, G_i has an elementary abelian normal q_i-subgroup $H_i \neq 1$, such that $G_i = G_{i-1}H_i$, and G_{i-1} operates faithfully and irreducibly on H_i by conjugation.*

In this section we collect some lemmas useful for the construction and study of such a series.

First notice that the faithful operation of G_{i-1} on H_i implies:

$$G_{i-1} \cap H_i = 1, \qquad i = 1, 2, \ldots . \tag{1.1a}$$

So G_i is merely the split extension of H_i by G_{i-1}. Hence *if we are given a chain $1 = G_0 \subset G_1 \subset \cdots \subset G_n$ satisfying* (1.1), *and wish to extend it to G_{n+1}, we need only construct a faithful,*[1] *irreducible module over the group ring $GF(q_{n+1})[G_n]$.*

[1] Of course, "faithful" means "faithful for G_n", not "faithful for the ring."

481-1

To construct such a module, we use the following lemmas, in all of which $1 = G_0 \subset \cdots \subset G_n$ is a sequence satisfying (1.1), with $n > 0$:

(1.2) LEMMA. *H_n is the only minimal normal subgroup of G_n.*

Proof. Since G_{n-1} operates irreducibly on H_n, the latter is a minimal normal subgroup of G. If K is any normal subgroup not containing H_n, then $K \cap H_n = 1$. So $K \simeq K \cdot H_n/H_n$ is faithfully represented on H_n by conjugation. But $[K, H_n] \subseteq K \cap H_n = 1$. Hence $K = 1$.

(1.3) COROLLARY. *The only chief series of G_n is*

$$1 \subset H_n \subset H_n \cdot H_{n-1} \subset \cdots \subset H_n \cdot H_{n-1} \cdot \ldots \cdot H_1 = G_n .$$

(1.4) COROLLARY. *Let $\mathscr{M}$ be any G_n-module on which H_n acts nontrivially. Then $\mathscr{M}$ is a faithful G_n-module.*

(1.5) LEMMA. *Let λ be a linear character of H_n into some field k. Suppose that the centralizer C of λ in G_n has the property that $(C : H_n)$ is relatively prime to q_n. Then there is a unique linear character $\tilde{\lambda}$ of C into k satisfying:*

$$\tilde{\lambda}|_{H_n} = \lambda \tag{1.6a}$$

$$\tilde{\lambda}(x) = 1, \qquad \textit{for any } q_n'\textit{-element } x \textit{ of } C. \tag{1.6b}$$

Proof. C normalizes the kernel K of λ. And: $[C, H_n] \subseteq K$. So C/K must be a direct product $(H_n/K) \times L$, where $|L| = (C : H_n)$ is relatively prime to q_n. Define $\tilde{\lambda}$ by the chain of natural maps:

$$C \to C/K = (H_n/K) \times L \to H_n/K \xrightarrow{\lambda} k.$$

Obviously $\tilde{\lambda}$ satisfies (1.6).

Notation. Given any linear character χ of a group G into a field k, let $\mathscr{M}(\chi)$ denote a one-dimensional $k[G]$-module having χ as its character.

(1.7) LEMMA. *Let $\lambda, \tilde{\lambda}$ and k be as in Lemma* 1.5. *Then the induced $k[G_n]$-module $\mathscr{M}(\tilde{\lambda})|^{G_n}$ is irreducible.*

Proof. H_n is normal in G_n. So (1.6a) implies:

$$\mathscr{M}(\tilde{\lambda})|^{G_n}|_{H_n} \simeq \sum_{\sigma} \oplus \mathscr{M}(\lambda^{\sigma}) \tag{1.8}$$

where σ runs over coset representatives for C in G_n. The characters λ^{σ} are all distinct. So *any $k[H_n]$-submodule* of $\sum \oplus \mathscr{M}(\lambda^{\sigma})$ *must be a sum of various* $\mathscr{M}(\lambda^{\sigma})$'s (and not just isomorphic to such a sum).

Suppose $\mathcal{N}$ is a nonzero $k[G_n]$-submodule of $\mathcal{M}(\tilde{\lambda})|^{G_n}$. Then the image of $\mathcal{N}$ under the isomorphism (1.8) contains at least one $\mathcal{M}(\lambda^\sigma)$. Since G_n permutes the corresponding subspaces of $\mathcal{M}(\tilde{\lambda})|^{G_n}$ transitively, $\mathcal{N}$ must contain them all. So $\mathcal{N} = \mathcal{M}(\tilde{\lambda})|^{G_n}$.

2. The Construction

We shall construct groups $1 = G_0 \subset G_1 \subset \cdots \subset G_5$ satisfying (1.1). The primes $q_1, ..., q_5$ will be chosen as follows:

$$q_1 = q_3 = q_5 = p, \qquad \textit{an odd prime} \tag{2.1a}$$

$$q_2 \mid p - 1 \tag{2.1b}$$

$$p \mid q_4 - 1. \tag{2.1c}$$

Evidently q_2 and q_4 can always be found once p is given.

$G_1 = H_1$ must be a cyclic group of order p. Evidently $1 = G_0 \subset G_1$ satisfies (1.1). For the further steps in the construction we need only provide faithful, irreducible $GF(q_{n+1})[G_n]$-modules $\mathcal{M}_{n+1}$, for $n = 1, 2, 3, 4$.

Let e be the smallest positive integer such that $q_2^e \equiv 1 \pmod{p}$. For $\mathcal{M}_2$ we take the additive group of $GF(q_2^e)$ on which a generator of G_1 operates as multiplication by a primitive pth root of 1 in $GF(q_2^e)$. Clearly $\mathcal{M}_2$ is a faithful irreducible $GF(q_2)[G_1]$-module.

Because of (2.1b), there is a nontrivial character λ_3 of H_2 into $GF(p)$. Clearly $H_2 = C_{G_2}(\lambda_3)$. So Lemma 1.7 tells us that:

$$\mathcal{M}_3 = \mathcal{M}(\lambda_3)|^{G_2} \tag{2.2}$$

is an irreducible $GF(p)[G_2]$-module. H_2 operates nontrivially on $\mathcal{M}_3$. So Corollary 1.4 implies that $\mathcal{M}_3$ is faithful.

From (1.8) we know the structure of H_3 as an H_2-group. Using the chain of natural maps:

$$H_3 \xrightarrow{\simeq} \mathcal{M}_3 \xrightarrow{\simeq} \sum_\sigma \oplus \mathcal{M}(\lambda_3^\sigma) \to \mathcal{M}(\lambda_3)$$

and an isomorphism of $\mathcal{M}(\lambda_3)^+$ into the multiplicative group of $GF(q_4)$ (which exists by (2.1c)), we construct a nontrivial character λ_4 of H_3 into $GF(q_4)$.

Let $C = C_{G_3}(\lambda_4)$. By construction $C \cap H_2$ is precisely the kernel of λ_3. Since $e > 1$, this is a nontrivial subgroup of H_2. If $C \cap G_2$ contained any element not in H_2, it would contain a conjugate of G_1. But any such conjugate would act irreducibly on H_2, and could not leave $C \cap H_2$ invariant. Hence

$C \cap G_2 = C \cap H_2$. So $(C : H_3) = ((C \cap H_2) \cdot H_3 : H_3) = | C \cap H_2 | = q_2^{e-1}$ is relatively prime to $q_3 = p$.

Now Lemmas 1.5 and 1.7 apply, giving us an irreducible $GF(q_4)[G_3]$-module $\mathcal{M}_4 = \mathcal{M}(\tilde{\lambda}_4)|^{G_4}$. By construction, H_3 operates nontrivially on $\mathcal{M}_4$. So Corollary 1.4 implies that $\mathcal{M}_4$ is faithful.

Let f be the smallest positive integer such that $p^f \equiv 1 \pmod{q_4}$. Define the character λ_5 on H_4 to $k = GF(p^f)$ by:

$$H_4 \xrightarrow{\simeq} \mathcal{M}_4 \xrightarrow{\simeq} \sum \oplus \mathcal{M}(\lambda_4^\sigma) \to \mathcal{M}(\lambda_4) \xrightarrow{\lambda} k \tag{2.3}$$

where λ is an isomorphism of $\mathcal{M}(\lambda_4)^+$ into the multiplicative group of k. Since $G_3 \simeq G_4/H_4$ is a p, q_2-group, and $q_4 \neq p, q_2$, the conditions of Lemma 1.5 are satisfied. So Lemma 1.7 gives us an irreducible $k[G_4]$-module $\mathcal{M} = \mathcal{M}(\tilde{\lambda}_5)|^{G_4}$. Let $\mathcal{M}, \mathcal{M}', \mathcal{M}'', \ldots$ be a complete set of distinct conjugate modules over $k[G_4]$ (where the conjugation leaves only $GF(p)$ fixed). Then there is an irreducible $GF(p)[G_4]$-module $\mathcal{M}_5$ satisfying:

$$\mathcal{M}_5 \otimes k \simeq \mathcal{M} \oplus \mathcal{M}' \oplus \cdots, \quad \textit{as } k[G_4]\textit{-modules.} \tag{2.4}$$

Since H_4 operates nontrivially on $\mathcal{M}$, it operates nontrivially on $\mathcal{M}_5$. As before, Corollary 1.4 implies that $\mathcal{M}_5$ is faithful.

3. The Structure of Sylow Subgroups

First we consider a Sylow p-subgroup of G_5:

(3.1) Proposition. *We adopt the notation of Section 2. Then G_5 has a p-Sylow subgroup S with the following structure:*

(3.2a) $S = H_1 \cdot H_3 \cdot H_5$.

(3.2b) *H_1 is cyclic of order p, normalizing both H_3 and H_5.*

(3.2c) *H_3 is elementary abelian of order p^p, normalizing H_5.*

(3.2d) *$H_1 \cap H_3 = 1$ and H_1 operates regularly on H_3 by conjugation.*

(3.2e) *H_5 is elementary abelian and $H_1 \cdot H_3 \cap H_5 = 1$.*

(3.2f) $\prod_{\tau \in H_3} x^\tau = 1$, *for all $x \in H_5$.*

Proof. By (1.1), H_1 normalizes H_3 and H_5, and H_3 normalizes H_5. Hence $H_1 \cdot H_3 \cdot H_5$ is a subgroup of G_5. From (2.1), we see that it is a Sylow p-subgroup. So (3.2a) holds.

By construction $H_1 = G_1$ is cyclic of order p. So (3.2b) holds.

Definition (2.2) implies that $| H_3 | = p^p$, and that H_1 operates regularly on H_3 by conjugation. By (1.1a), $H_1 \cap H_3$ is 1. So (3.2c) and (3.2d) hold.

(3.2e) is implied by (1.1) and (1.1a).

The critical fact is (3.2f). This is equivalent to:

$$\sum_{\tau \in H_3} \tau(m) = 0, \textit{ for all } m \in \mathcal{M}_5 .$$

In view of (2.4), this is equivalent to:

$$\sum_{\tau \in H_3} \tau(m) = 0, \textit{ for all } m \in \mathcal{M}. \tag{3.3}$$

We need only prove (3.3) for a set of m spanning $\mathcal{M}$. To form such a set, we use (1.8). Let $\tilde{m}_\sigma$ be a generator for $\mathcal{M}(\lambda_5^\sigma)$, and let m_σ be the corresponding element of $\mathcal{M}$. It is evident from (2.3) that $C_{G_4}(\lambda_5^\sigma) \cap H_3 = [C_{G_4}(\lambda_5) \cap H_3]^\sigma = \operatorname{Ker}(\lambda_4)^\sigma$, provided that σ is chosen from G_3 (which is always possible). But $\operatorname{Ker}(\lambda_4)^\sigma$ has order p^{p-1}. Hence:

$$\sum_{\tau \in \operatorname{Ker}(\lambda_4)^\sigma} \tau(m_\sigma) = p^{p-1} \cdot m_\sigma = 0 \textit{ in } \mathcal{M}.$$

So we certainly must have (3.3) for $m = m_\sigma$. The m_σ's span $\mathcal{M}$. So (3.3) holds in general.

We also need some information about a Sylow p-subgroup Σ of the symmetric group on p^3 letters.

(3.4) PROPOSITION. *Σ has subgroups Σ_1, Σ_3, Σ_5 satisfying:*

(3.5a) $\Sigma = \Sigma_1 \cdot \Sigma_3 \cdot \Sigma_5$.

(3.5b) *Σ_1 is cyclic of order p, normalizing both Σ_3 and Σ_5.*

(3.5c) *Σ_3 is elementary abelian of order p^p, normalizing Σ_5.*

(3.5d) *$\Sigma_1 \cap \Sigma_3 = 1$ and Σ_1 operates regularly on Σ_3 by conjugation.*

(3.5e) *Σ_5 is elementary abelian of order $p^{p^{1+p}}$, and $\Sigma_1 \cdot \Sigma_3 \cap \Sigma_5 = 1$.*

(3.5f) *$\Sigma_1 \cdot \Sigma_3$ operates regularly on Σ_5 by conjugation.*

Proof. All these properties follow immediately from the fact (see [*1*]) that Σ is the wreath product $Z_p \wr Z_p \wr Z_p$ of three cyclic groups of order p.

(3.6) LEMMA. *Σ_5 is the only maximal normal abelian subgroup of Σ.*

Remark. This is not true if $p = 2$.

Proof. Σ_5 is a normal abelian subgroup of Σ by (3.5b, c, e). Let A be any normal abelian subgroup. Then $[A, \Sigma_5] \subseteq A$. Hence $[A, [A, \Sigma_5]] = 1$. So the minimal polynomial of the transformation on Σ_5 induced by conjugation by an element of A must divide $(X - 1)^2$. On the other hand, (3.5f) implies that the corresponding minimal polynomial for any element of Σ not in Σ_5 is divisible by $(X - 1)^p$. Since $p \geqslant 3$, we conclude that $A \subseteq \Sigma_5$.

4. The Nonexistence of H, K

Now we can demonstrate that G_5 answers the question (0.1).

(4.1) Theorem. *G_5 is p-solvable of p-length 3. It does not contain any subgroups H, K such that K is normal in H and H/K is isomorphic to Σ.*

Proof. By Corollary 1.3, G_5 has only one chief series, whose factors are, in order, H_1, H_2, H_3, H_4, H_5. Since H_1, H_3, H_5 are p-groups, while H_2, H_4 are p'-groups, it is clear that G_5 is p-solvable of p-length 3.

Suppose the above groups H, K did exist. We may assume that H is contained in the p-Sylow subgroup S of G_5. Let ϕ be a homomorphism of H onto Σ having K as its kernel.

H_5 is a normal abelian subgroup of S. Hence $\phi(H \cap H_5)$ is a normal abelian subgroup of $\phi(H) = \Sigma$. From lemma 3.6, we conclude that:

$$\phi(H \cap H_5) \subseteq \Sigma_5. \tag{4.2}$$

On the one hand:

$$H/H \cap H_5 \simeq H \cdot H_5/H_5 \subseteq S/H_5 \simeq H_1 \cdot H_3. \tag{4.3}$$

On the other:

$$H/H \cap H_5 \to H/K(H \cap H_5) \simeq \phi(H)/\phi(H \cap H_5) \to \Sigma/\Sigma_5 \simeq \Sigma_1 \cdot \Sigma_3 \tag{4.4}$$

where all homomorphisms are onto. But (3.2b, c) and (3.5b, c) tell us that $H_1 \cdot H_3$ and $\Sigma_1 \cdot \Sigma_3$ both have order p^{1+p}. So *equality holds in* (4.2) *and* (4.3), *and the homomorphisms in* (4.4) *are all isomorphisms.*

By (3.5f) there must be an element σ_5 of Σ_5 satisfying:

$$\prod_{\tau \in \Sigma_1 \cdot \Sigma_3} \sigma_5{}^\tau \neq 1. \tag{4.5}$$

Since equality holds in (4.2), there is an element h_5 in H_5 satisfying: $\phi(h_5) = \sigma_5$. For each $\tau \in \Sigma_1 \cdot \Sigma_3$, choose an element τ' in H satisfying $\phi(\tau') = \tau$. Then (4.5) implies:

$$\prod_{\tau \in \Sigma_1 \cdot \Sigma_3} h_5^{\tau'} \neq 1. \tag{4.6}$$

The elements τ' are coset representatives of $\phi^{-1}(\Sigma_5) = K \cdot (H \cap H_5)$ in H. Since the first homomorphism in (4.4) is an isomorphism, $K \cdot (H \cap H_5) = H \cap H_5$. So the τ' are coset representatives of H_5 in $H \cdot H_5$. But equality holds in (4.3). Hence the τ' are coset representatives of H_5 in S. We conclude that:

$$\prod_{\tau \in \Sigma_1 \cdot \Sigma_3} h_5^{\tau'} = \prod_{\rho \in H_1 \cdot H_3} h_5{}^{\rho} = \prod_{\rho_1 \in H_1} \left[\prod_{\rho_3 \in H_3} h_5^{\rho_3} \right]^{\rho_1}.$$

By (3.2f) the last product is 1. This contradicts (4.6), and proves the theorem.

References

1. Hall, Jr., M., "The Theory of Groups," pp. 81-83. Macmillan, New York, 1959.
2. Hall, P., and Higman, G., The p-length of a p-soluble group, and reduction theorems for Burnside's problem. *Proc. London Math. Soc.* (3) **6** (1956), 8.